

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA)	
)	Docket No. 20-cr-10012-IT
)	
v.)	
)	
)	
PAUL BATEMAN)	

**DEFENDANT’S MOTION TO RECONSIDER THE COURT’S ORDERS DENYING
DEFENDANT’S MOTION TO SUPPRESS AND MOTION TO COMPEL**

EXHIBIT 1:

Application for Search Warrant
20-mj-00481-SJB (W.D. Mich. Nov. 19, 2020)

UNITED STATES DISTRICT COURT

for the
Western District of Michigan

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

The entire premises located at 234 South Magnolia
Avenue, Lansing, Michigan 48912, further described in
Attachment A.

Case No. 1:20-MJ-481

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ Western _____ District of _____ Michigan _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

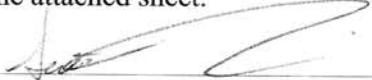
Code Section	Offense Description
18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B)	Receipt and distribution of child pornography; Access with intent to view child pornography.

The application is based on these facts:

See Attached Continuation.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

SA Scott J. Robinson, FBI


Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

Telephone _____ (specify reliable electronic means)

Date: November 19, 2020

City and state: Grand Rapids, Michigan


Judge's signature

Hon. Sally J. Berens, United States Magistrate Judge

Printed name and title

**CONTINUATION IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Scott Robinson, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the FBI since 2019 and am currently assigned to the Detroit Division. My duties include the investigation of alleged violations of federal criminal laws, including the subject offense, sexual exploitation of children (18 U.S.C. §§ 2251 and 2252A).

2. This continuation is submitted in support of an application, under Rule 41 of the Federal Rules of Criminal Procedure, for a search warrant for the locations specifically described in Attachment A, including the entire property located at **234 S Magnolia Avenue, Lansing, Michigan 48912** (the “SUBJECT PREMISES”) and the content of electronic storage devices located therein, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (access with intent to view child pornography), which items are more specifically described in Attachment B.

3. The statements contained in this continuation are based in part on information provided by U.S. federal law enforcement agents, written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information

gathered from investigative sources of information, and my experience, training and background as a Special Agent.

4. This continuation is submitted for the limited purpose of securing a search warrant. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of federal law are located at the SUBJECT PREMISES.

SUMMARY OF INVESTIGATION

5. A user of the internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography. The child pornography is housed on a website operated on the Tor anonymity network.

I. The Tor Network

6. The internet is a global network of computers and other devices. Devices directly connected to the internet are uniquely identified by IP addresses. IP addresses are used to route information between internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address. This way, the responding device knows where to send its response. On the internet, data transferred between devices is split into discrete packets, each of which has two parts: (1) a header with non-content routing and control information, such as the packet's source and destination IP addresses;

and (2) a payload, which generally contains user data or the content of a communication.

7. TARGET WEBSITE operated on the Tor network. The Tor network is a computer network, available to internet users, that is designed specifically to facilitate anonymous communication over the internet. The Tor network routes communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a “circuit.” Because of the way the Tor network routes communications through the relay computers, traditional techniques to identify a user’s IP address are not effective.

8. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free “Tor browser” from the Tor Project, the private entity that maintains the Tor network, via their website. The Tor browser is a web browser that is configured to route a user’s internet traffic through the Tor network.

9. As with other internet communications, a Tor user’s communications are split into packets containing header information and a payload, and those communications are routed using IP addresses. In order for a Tor user’s communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user’s IP address with Tor network relay computers, which are called “nodes.” This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next

node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

10. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses an internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the content of a Tor user's communications are encrypted while the communication passes through the Tor network. The encryption prevents the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

11. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?" is asked, to which the response is, in bold text, "No."

12. The Tor Network also makes it possible for users to operate websites, such as those described herein, called "hidden services" or "onion services," in a

manner that attempts to conceal the true IP address of the computer hosting the website. Hidden service websites are accessible only to users operating within the Tor network. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.

13. Unlike standard internet websites, a Tor-based web address is comprised of a series of at least 16 and as many as 56 algorithm-generated characters, for example "asdlk8fs9dfku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. There is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. While law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

II. Description of TARGET WEBSITE

14. The conduct being investigated involves users of a Tor-network-based website; TARGET WEBSITE. The TARGET WEBSITE was an online bulletin board dedicated to the advertisement and distribution of child pornography that operated from approximately at least September 2016 to June 2019. In June of 2019, the computer server hosting the TARGET WEBSITE, which was located outside of the United States, was seized by a foreign law enforcement agency.

15. A review of the initial TARGET WEBSITE page revealed it was a message board web page that contained a search bar, and showcased two hyperlinks titled, “Announcements” and “Important Information.” Located below the title were hyperlinks including those entitled “Quick Links,” “Home,” “Board Index,” “Login,” and “Register.” As of June 2019, the website had over 820,000 members and over 81,000 postings.

16. Upon accessing the “Announcements” hyperlink of the TARGET WEBSITE, the following message was displayed in message board form, “Welcome, Please read before registering” which was dated July 1, 2016. Upon accessing the aforementioned hyperlink, the message read, “Welcome abusers and abusees and those that enjoy watching. This website was created to host videos, photos and discussions of 18 (twinks) and younger of Hurtcore materials (videos & pictures) as well as discussion of such.” Based on my training and experience, I know that

Hurtcore refers to violent pornography. The message continued, “PS Please register to see all the forums, and use strong password for user profile.”

17. Upon accessing the “Register” link of the TARGET WEBSITE, it was revealed that users would complete a “Username,” “Password,” “Confirm password,” “Language,” and “My timezone,” fields, as well as a “Confirmation of Registration” code. Upon entering the TARGET WEBSITE, sections and forums for posting to the website included “HURTCORE Toddlers Videos (Ages 0-5),” “Preteen/Hebe Children Videos (Ages 6-13),” “Teens Videos (Ages 14+),” “Toddlers Images (Ages 0-5),” “Preteen/Hebe Children Images (Ages 6-13),” and “Teens Images (Ages 14+).” Based on my training and experience, I know that “Hebe” is a reference to a “hebephile,” which is a person with a persistent sexual interest in pubescent minor children. Another forum was named “GORE/DEATH” which included sub-forms for “Toddlers (Ages 0-5),” “Preteen/Hebe Children (Ages 6-13)” and “Teens (Ages 14+).” An additional section of the website called “The Team” listed the usernames of two website “Administrators” and five “Global Moderators.” The TARGET WEBSITE also contained a private message feature that was available, allowing users to send private messages to each other.

18. On June 23, 2016, a website administrator posted a topic entitled “Board Rules” in the “Important Information” forum which contained the following explanation of the website:

Rules are simple all material must be related to Hurtcore content. What is Hurtcore content? It is rape, fighting, wrestling, bondage, spanking,

pain, mutilation, gore, dead bodies, and etc. (no limits) Why does this place exist? There was a need and since society thinks I am worst than any abuser or creator of Hurtcore content, I decided to create this place for those who like it and want to share. Besides I am the mischievous god. It is up to you to make this the best Hurtcore board there is. So please upload whatever you can so that it can be shared.

19. A review of the “Toddlers Videos,” “Preteen/Hebe Children,” “Toddlers Images,” and “Gore/Death” forums and subforums, as well as additional forums, within the various above sections revealed they contained numerous pages of topics. Each topic contained a title, the author, the number of replies, the number of views, and the last post. The last post section included the date and time of the post as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the thread below it. Typical posts appeared to contain text, images, thumbnail previews of images, links to external sites with compressed files (such as “.rar”), or replies to previous posts.

20. A review of topics within these sections revealed numerous posts containing images and/or videos depicting child pornography and child erotica of prepubescent males, females, toddlers, and infants; including those depicting anal, vaginal, and oral penetration. Additionally, these sections revealed numerous posts containing images and/or videos depicting child pornography involving gore and sometimes death. Examples of these are as follows:

- a. On October 9, 2016, a website user posted a topic entitled “Fuck the newborn. Real fuck!” in the “Hurtcore/Toddlers Images/Girls” forum, that contained nine

images depicting child pornography and child erotica of a prepubescent female infant. One of these images depicted a naked female infant lying on her back with her legs spread apart, exposing her vagina, with a gloved adult finger inserted into her anus. A male's penis was pressed against her vagina and the head of the penis inserted into her mouth. A brown liquid substance, appearing to be the infant's feces are seen smeared around her anus.

- b. On November 5, 2016, a website user posted a topic entitled "BabyHee 1yo (one of full version)" in the "HurtCore/Toddlers Videos/Boys" forum that contained images depicting child pornography and torture of a prepubescent male, who was completely naked and tied down with rope on the side of a bath tub. Among other things, the images depicted an adult male defecating on the chest and urinating in the mouth of the prepubescent male.

III. Hidden Service Websites and TARGET WEBSITE

21. As described herein, TARGET WEBSITE could not generally be accessed through the traditional internet. Only a user who had installed the appropriate Tor software could access TARGET WEBSITE. Even after connecting to the Tor network, a user would have to find the 16-character web address of TARGET WEBSITE in order to access it. Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—like websites that operate on the open internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open internet websites for a particular

content of interest. Users interested in accessing child exploitive material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain and use directory sites that advertise the web addresses of hidden services that contain child exploitative related content. Those directory sites also operate via the Tor network.

22. Users utilize directory sites to identify new web forums, chat sites, image galleries, and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are operating, whether images of child pornography imagery may be found there, and even what types of child pornography are accessible (i.e., boys, girls, or “hurtcore”). They also contain clickable hyperlinks to access those sites. As with other hidden service websites, a user must find the 16-or-56 character web address for a directory site in order to access it. While it operated, the web address for TARGET WEBSITE was listed on one or more of these directory sites advertising hidden services dedicated to the sexual exploitation of children.

23. Based on my training and experience, because accessing TARGET WEBSITE required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via Tor – it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content.

24. Based on my training and experience, I know that it is extremely rare for an individual who takes the numerous positive steps to find child pornography on a Tor hidden services website to only visit that website one time. One example of this is analysis of “Playpen”, which was a Tor network-based hidden service dedicated to the advertisement and distribution of child pornography that operated from August 2014 until March 2015. Similar to TARGET WEBSITE, Playpen was a highly categorized web forum with hundreds of thousands of users. It allowed users to post and download messages pertaining to child exploitation within forum categories. The categories were indexed by the age and gender of child victims and the type of sexual activity involved. In February and March of 2015, the FBI seized and briefly operated the Playpen website for two weeks, using a court-authorized investigative technique to successfully identify IP addresses and other information associated with site users. The FBI’s review of site data seized from the Playpen website during the operation determined that, of over 400,000 total user accounts observed on the Playpen website during its existence, less than 0.02 percent (that is, less than two hundredths of one percent) of user accounts with a registered account on the website accessed a message thread on the website only once.

25. Probable cause exists that any user who accessed TARGET WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so.

26. U.S. and foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor hidden service websites such as TARGET WEBSITE and other websites described herein. Those websites are globally accessible. The websites and their users may be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located. Accordingly, when a law enforcement agency obtains evidence that such a website or website user may be located in another country, in accordance with each country's laws, it is common practice for that law enforcement agency to share information with law enforcement (1) in the country where the site is located; or (2) where the offender appears to reside.

27. In August of 2019, a Foreign Law Enforcement Agency (referenced herein as "FLA") known to the FBI, and with a history of providing reliable, accurate information in the past, contacted the FBI. The FLA provided the following information:

28. On May 14, 2019, at 19:52:14 UTC¹, a user of IP address 52.144.38.57 accessed online child sexually abusive and exploitive material via a website on the Tor network, the TARGET WEBSITE;

¹ UTC is Coordinated Universal Time; it is five hours ahead of Eastern Standard Time.

- a. The website was described as having “*an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on BDSM, hurtcore, gore and death-related material including that of children,*”;
- b. “[u]sers were required to create an account (username and password) in order to access the majority of the material,”; and
- c. documentation naming TARGET WEBSITE, which the FLA referred to by its actual name.

29. According to publicly available information, IP address 52.144.38.57 was registered to Lightspeed Communications.

30. On January 3, 2020, through a subpoena, the FBI determined that Lightspeed Communications IP address 52.144.38.57 resolved to Nicole Hope, **234 S Magnolia Avenue, Lansing, Michigan 48912**, which is the address of the SUBJECT PREMISES.

31. A search of a public records database for the SUBJECT PREMISES revealed that, since approximately 2018, Nicole Hope, date of birth January 19, 1983, is likely the current resident. Daniel Conlin Jr., date of birth August 11, 1987, is also a likely resident. Records from the Michigan Secretary of State showed that Nicole Hope and Daniel Conlin Jr. have driver’s licenses that list the home addresses as the SUBJECT PREMISES.

32. On August 3, 2020, the U.S. District Court for the Western District of Michigan authorized the installation and use of a pen register/trap and trace device (PRTT) to record, decode and/or capture all dialing, routing addressing and signaling information associated with each communication to or from the residential internet service account associated with the SUBJECT PREMISES provided by Lightspeed Communications. A renewal of the PRTT was authorized on September 17, 2020.

a. Based on my training and experience, I am aware that analysis of data obtained via a PRTT on a target's residential internet connection can provide evidence that a user of the internet at the premises is accessing the Tor network. That is possible because the IP addresses of Tor node computers that make up the network are published by the Tor network. Since a residential internet PRTT will disclose the IP addresses of computers to which communications are sent and from which communications are received, analysis of the PRTT data can reveal Tor use. Due to Tor routing and encryption, a PRTT will not reveal the ultimate destination or the content of those communications.

b. Lightspeed Communications began to provide data for this PRTT on September 15, 2020. Analysis through November 16, 2020 of the data provided pursuant to that PRTT order revealed evidence that a user of the internet at the SUBJECT PREMISES accessed the Tor network on eight separate days since Lightspeed Communications started providing data:

- i. September 16, 2020 at 6:49 a.m.;
- ii. September 26, 2020 at 11:04 p.m.
- iii. October 31, 2020 at 1:09 p.m.
- iv. November 9, 2020 at 11:25 p.m.
- v. November 10, 2020 at 1:05 p.m.
- vi. November 12, 2020 at 1:22 p.m. and 2:33 p.m.
- vii. November 13, 2020 at 5:58 p.m.
- viii. November 15, 2020 at 11:44 a.m., 1:16 p.m., and 1:58 p.m.²

33. Based on my training and experience, although the TARGET WEBSITE is no longer in service, the fact that an internet user at the SUBJECT PREMISES continue to access the Tor network means that it is likely the user is continuing to use the Tor network for child exploitation purposes. While I know that the Tor network contains sites other than those involving child pornography, I know based on my training and experience that the Tor network contains many sites dedicated to child pornography and child exploitation, just like the TARGET WEBSITE, and individuals that seek out child pornography will continue to do so even if a website they have utilized in the past is no longer in service.

² All times listed in this paragraph are in Eastern Standard Time.

IV. The Foreign Law Enforcement Agency

34. The FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of reciprocal criminal investigative cooperation between U.S. law enforcement and the FLA. This cooperation includes the investigation of crimes against children. The FLA advised U.S. law enforcement that it obtained the information through an independent investigation that was lawfully authorized in the FLA's country pursuant to its national laws. Further, the FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to obtain the 52.144.38.57 IP address information. U.S. law enforcement personnel did not participate in the investigative work through which the FLA identified the 52.144.38.57 IP address provided by the FLA.

35. I am aware through my training and experience, and through consultation with other U.S. law enforcement agents, that tips provided by the FLA, regarding IP addresses that the FLA advised were associated with access to Tor network child exploitation-related web and chat sites, have: (1) led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to

be related to targets that U.S. law enforcement investigations had independently determined were associated with the trafficking and possession of child pornography.

Background on Child Pornography, Computers, and the Internet

36. Based on my training, experience, and information obtained from other agents, I know the below statements are accurate.

37. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

38. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as WiFi or Bluetooth. Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

39. Any computer can connect to any smartphone, tablet, or other computer. Through the internet, electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

40. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

41. The internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

42. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the internet. Even in cases where online storage is used, however, evidence

of child pornography can be found on the user's computer, smartphone, or external media in most cases.

43. Individuals commonly use smartphone and computer apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

44. Communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Specifics Related to the Search and Seizure of Computer Systems

45. As described above and in Attachment B, this application seeks permission to search for evidence that exists in the SUBJECT PREMISES, in whatever form they are found. The evidence is likely to be found on and stored in a computer's hard drive or other storage media. Thus, the warrant applied for would

authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

46. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe the evidence referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file;

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data;

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic

evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information; and

d. Files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or “cache.”

47. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. Probable cause exists that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES.

48. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can

reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

49. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media.

50. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers

typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

51. Some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data also typically contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user.

52. Information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the

computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

53. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

54. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

55. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

56. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an

instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain data that is evidence of how the computer was used, data that was sent or received, notes as to how the criminal conduct was achieved, records of internet discussions about the crime, and other records that indicate the nature of the offense.

57. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises, it is not always possible to search computer equipment and storage devices for data for a number of reasons.

- a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search

site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched.

- b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.
- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises.
- d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension

“.jpg” often are image files. A user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text.

- e. Computer users can also attempt to conceal data by using encryption. Encryption involves the use of a password or device, such as a “dongle” or “keycard,” to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.
- f. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (an individual may access the wireless network without a key or password) wireless routers for both networks may yield

significant evidence of, or serve as instrumentalities of, a crime. This includes identifying the instrument through which the perpetrator of the internet-based crime connected to the internet. This may potentially contain logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

58. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium. This might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Request to Use Biometric Data to Unlock Devices

59. This warrant seeks to permit law enforcement to compel all residents of the SUBJECT PREMISES who are present at the SUBJECT PREMISES to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called

“Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

60. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are

considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

61. As discussed, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant are currently unknown to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

62. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features,

the opportunity to unlock the device through a biometric feature may exist for only a short time.

63. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of all residents of the SUBJECT PREMISES who are present at the SUBJECT PREMISES to the fingerprint scanner of the DEVICES found at the SUBJECT PREMISES; (2) hold the DEVICES found at the SUBJECT PREMISES in front of the face of all residents of the SUBJECT PREMISES who are present at the SUBJECT PREMISES and activate the facial recognition feature; and/or (3) hold the DEVICES found at the SUBJECT PREMISES in front of the face of all residents of the SUBJECT PREMISES who are present at the SUBJECT PREMISES and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that all individuals present at the SUBJECT PREMISES to state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel all individuals present at the SUBJECT PREMISES to identify the specific biometric characteristics (including the unique

finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

64. For the foregoing reasons, I submit that probable cause exists that contraband, property, evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (access with intent to view child pornography), more fully described in Attachment B, will be located at the locations described in Attachment A.

ATTACHMENT A
Locations to be Searched

The entire property located at 234 South Magnolia Avenue, Lansing, Michigan 48912, including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES) and vehicles present at the subject premises within the control of the residents of the SUBJECT PREMISES. The SUBJECT PREMISES are further identified as follows: 234 South Magnolia Avenue, Lansing, Michigan 48912 located on the west side of South Magnolia Avenue, between Prospect Street and East Michigan Avenue. The structure is a two-story family residence with white siding. The front door is red and the number 234 affixed to the left of the door. A white detached two-stall garage is located behind the residence. The residence is depicted below:



ATTACHMENT B
Items to be Seized and Searched

The following materials, which may constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § 2252A:

1. Computers and storage media

a. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

b. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. Evidence of who used, owned, or controlled the COMPUTER at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. Evidence of the lack of such malicious software;
- d. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- e. Evidence indicating the computer user’s knowledge and/or intent as it relates to the crime(s) under investigation;
- f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. Evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

- h. Evidence of the times the COMPUTER was used;
- i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. Records of or information about internet Protocol addresses used by the COMPUTER;
- l. Records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses; and
- m. Contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the internet.

4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

- a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence.
- b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for internet access, and handwritten notes.
- c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above.
- d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

6. As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

7. During the execution of the search of the SUBJECT PREMISES described in Attachment A, law enforcement personnel are also specifically

authorized to compel all residents of the SUBJECT PREMISES who are over the age of 15 and present at the SUBJECT PREMISES to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

- a. any of the DEVICES found at the SUBJECT PREMISES, and
- b. where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES's security features in order to search the contents as authorized by this warrant.

8. This warrant does not authorize law enforcement personnel to compel any other individuals found at the PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that any individuals present at the SUBJECT PREMISES state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

9. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.